RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: PART4-T02

The Future of the SOC in an AI-Driven Universe

Dave Gold
VP and Field CTO, SentinelOne

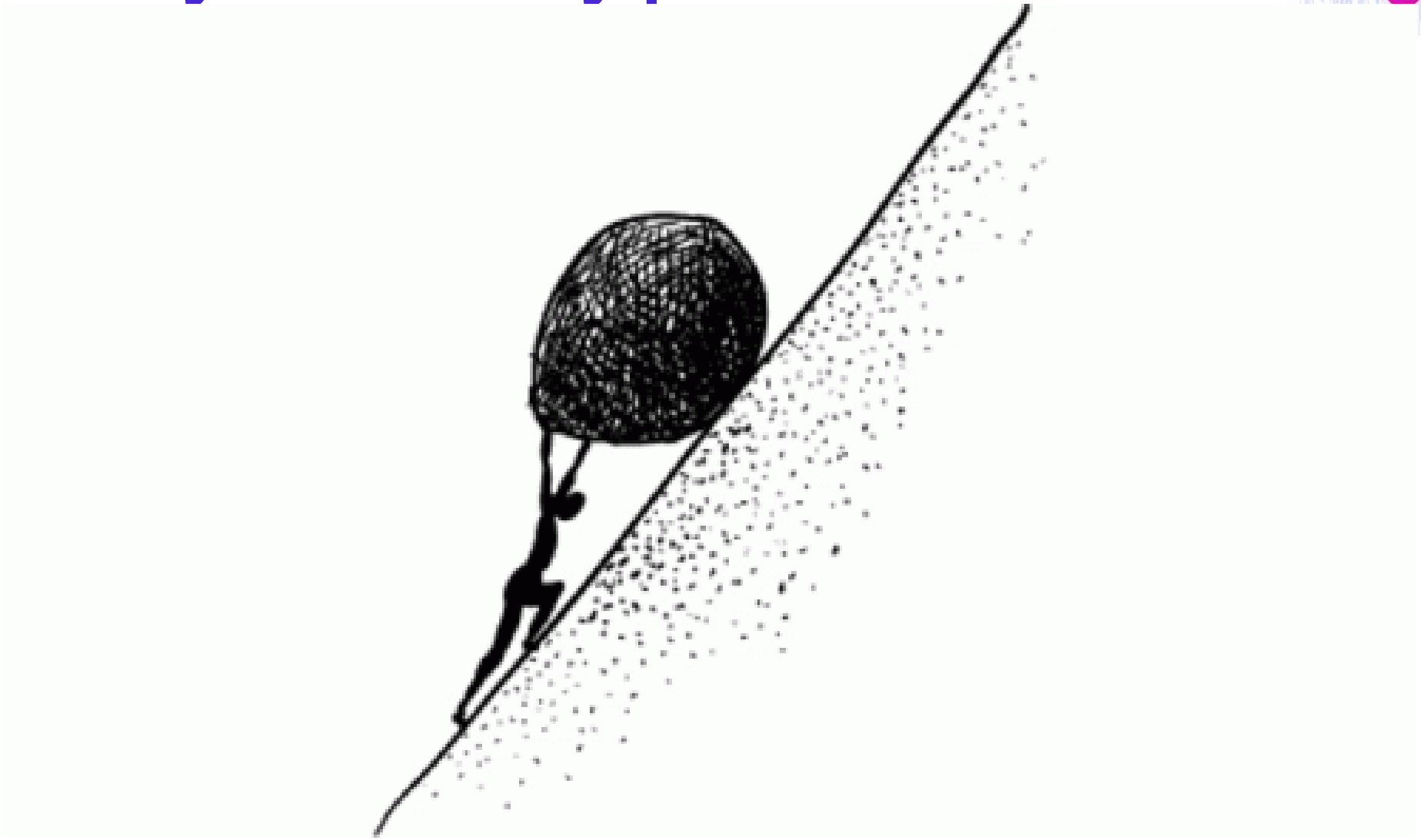
Agenda

- The Current State of the SOC
- The SOC of the Future
- Evolving the SOC

RSAC 2025 Conference

The Current state of the SOC

Life as a cybersecurity professional



The SOC – Under Resourced and Overloaded

SentinelOne

RSAC 2025 Conference

Security Is a data problem

SentinelOne

RSAC 2025 Conference

Too much to do, not enough time

Triage | Hunt & Investigate | Respond | Remediate | Proactive Risk Management

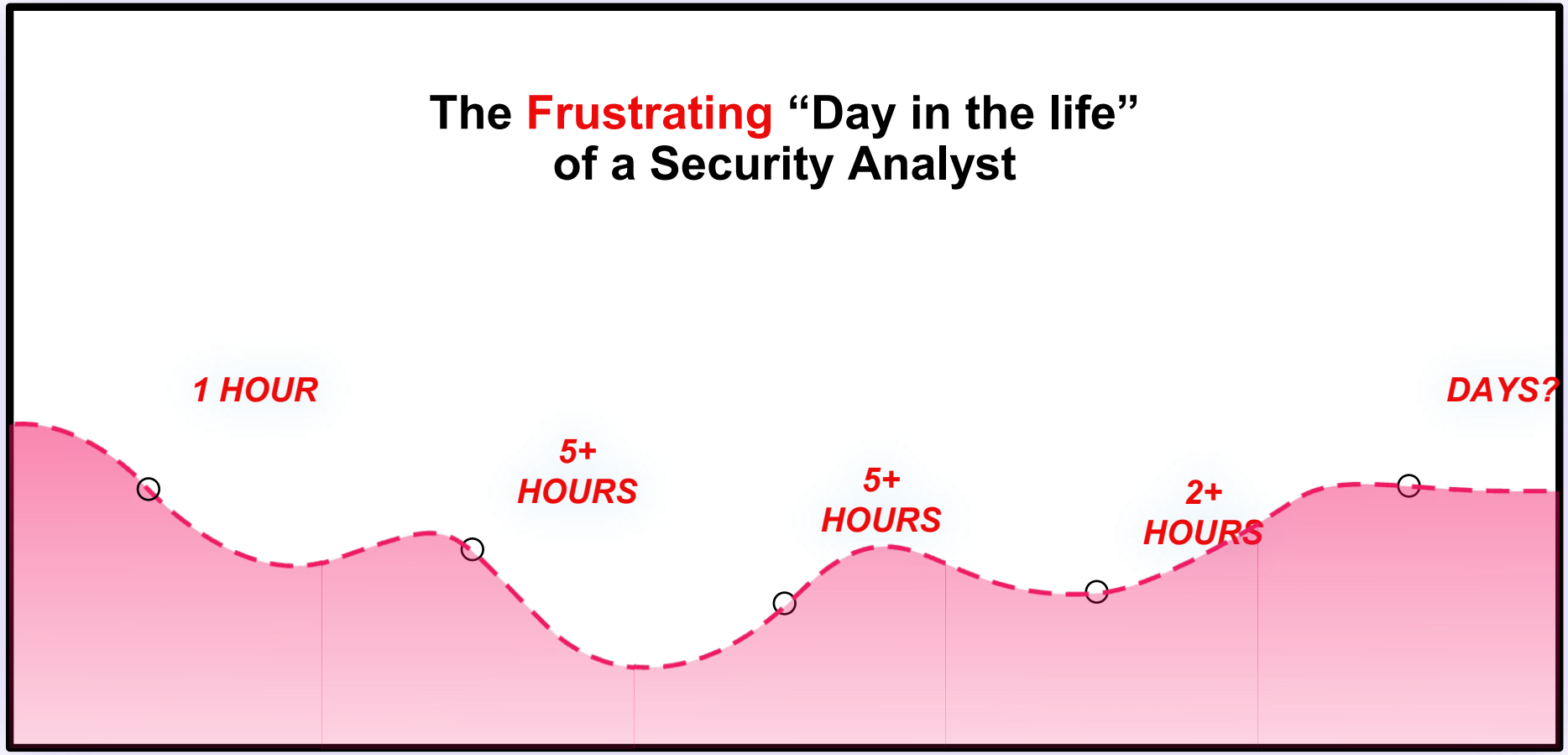
Very Happy

Happy

Neutral

Frustrated

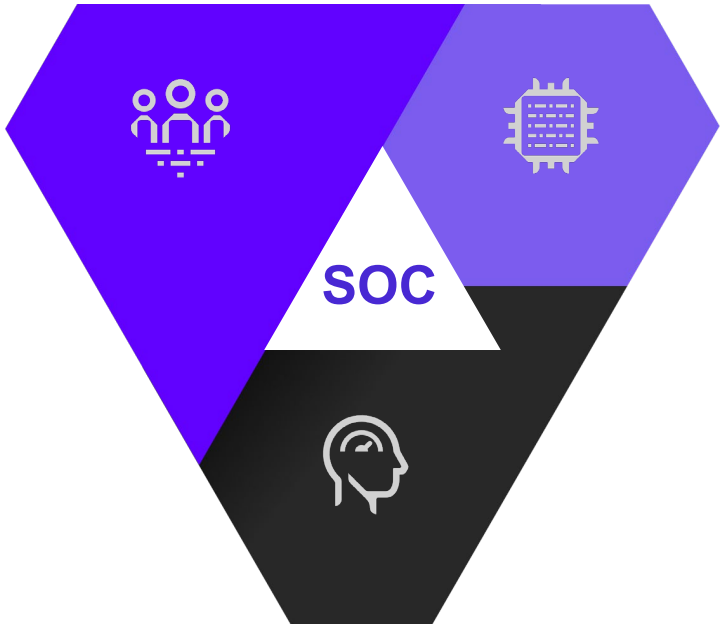
Very Frustrated



The SOC of Today

People

- Security Analysts
- Incident Responders
- Threat Hunters
- SOC Managers



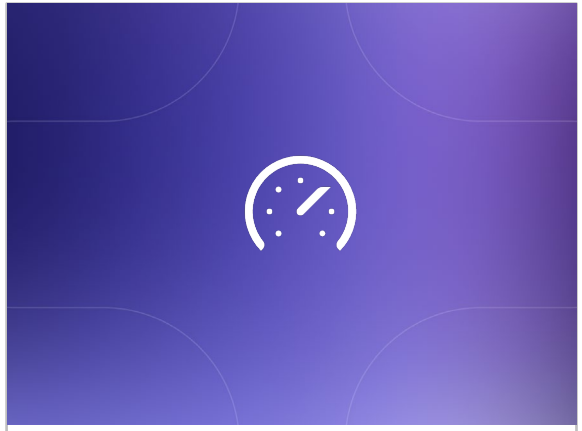
Technology

- SIEM
- SOAR
- EDR / XDR
- Threat Intel
- Case Management

Process

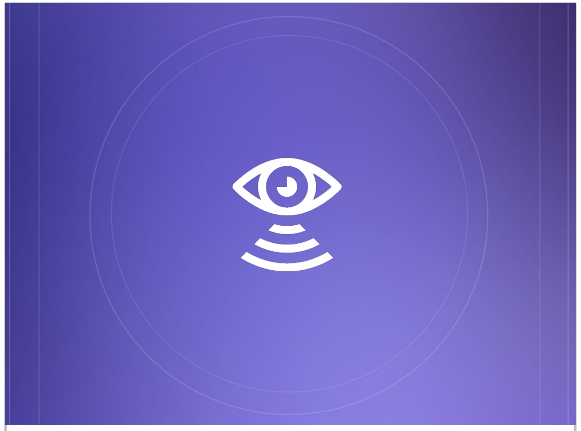
- Playbooks
- IR Procedures
- Compliance
- Frameworks

Same problems persist



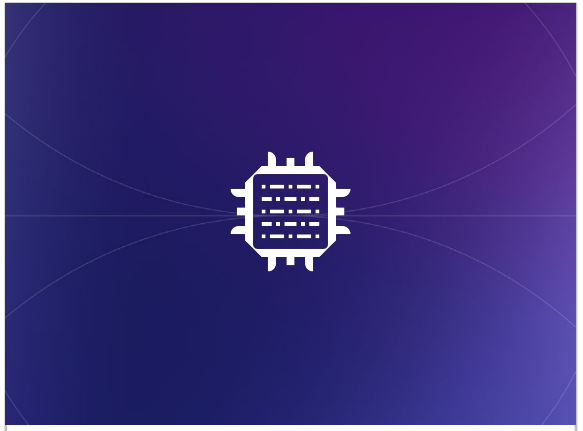
Slow & Manual

Legacy systems can’t keep up with the rapid evolution of threats. Lack of automation



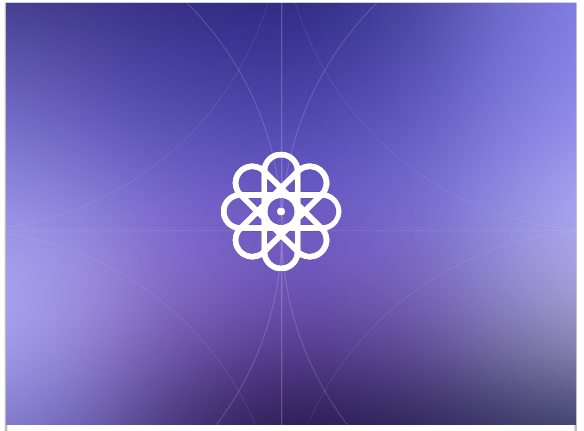
Limited Visibility

Blind spots and siloed solutions leave critical gaps in visibility. Especialy in the cloud



Too Much Noise

Alerts overwhelm security teams, leading to missed or delayed responses.



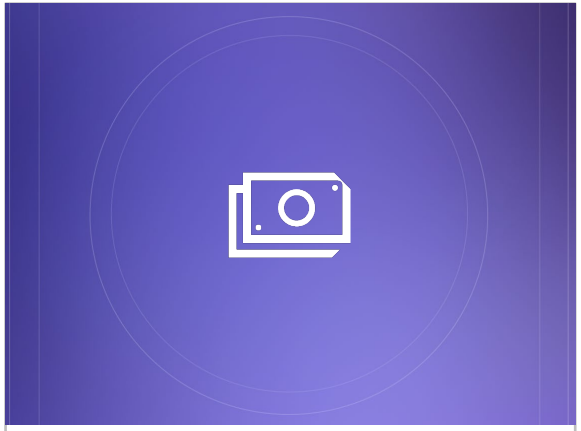
Cost & Complexity

Managing disparate tools and massive data repositories is expensive and resource intensive.

Why didn’t SIEM solve it?

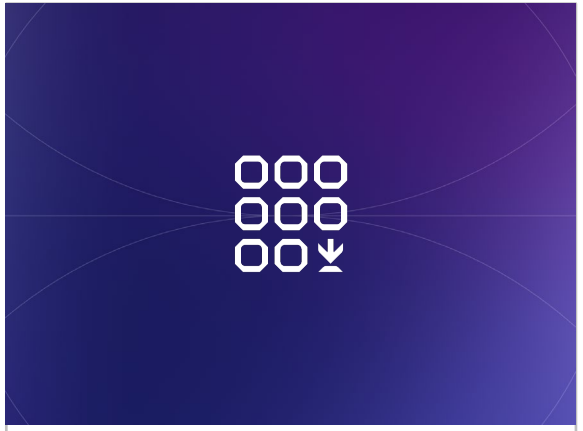
Scalability Issues

Traditional storage and analytics systems struggle to cope with the explosion of data. Cloud made it worse



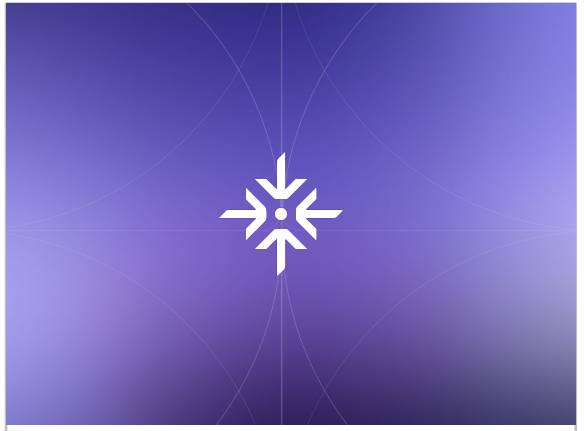
Cost Concerns

Retention and storage places financial strain often leading to trade-offs.



Flexibility and Integration

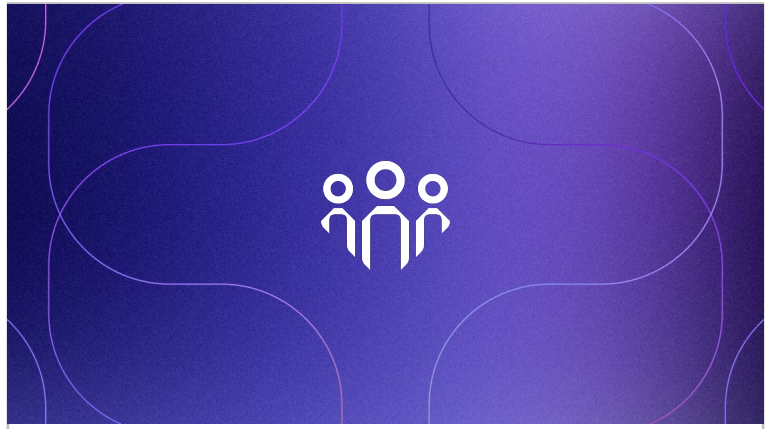
Difficulty to integrate traditional systems with modern operations.



Detection Content

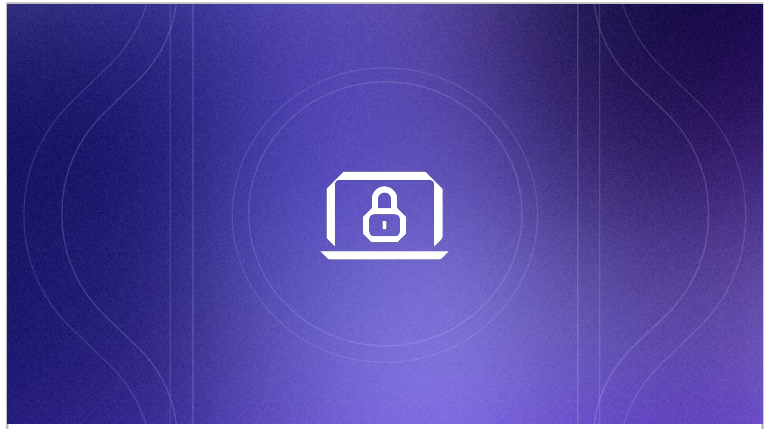
Hard to extract security value from the large amounts of siloed data

Why didn’t SOAR solve it?



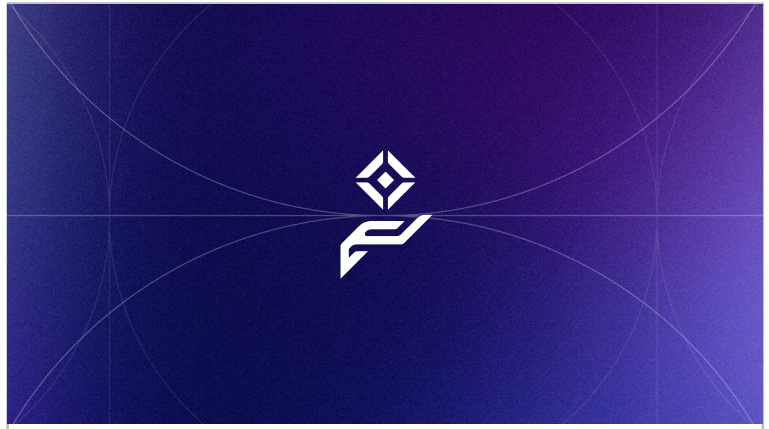
Complex implementation and Maintenance

SOAR platforms require substantial financial investment for both initial deployment and ongoing maintenance



Lack of scalability and Modernization

Legacy Architectures and lack of cloud and AI integration



Hard to Integrate

Adds another tool to operate and manage. Often relies on SIEM and is bolted-on. Doesn’t address data issues or skills gap

AI as a catalyst for change

SentinelOne

RSAC 2025 Conference

What will the SOC of the future look like?

SentinelOne

RSAC 2025 Conference

Agentic AI

SentinelOne

RSAC 2025 Conference

Augmented and Virtual Reality

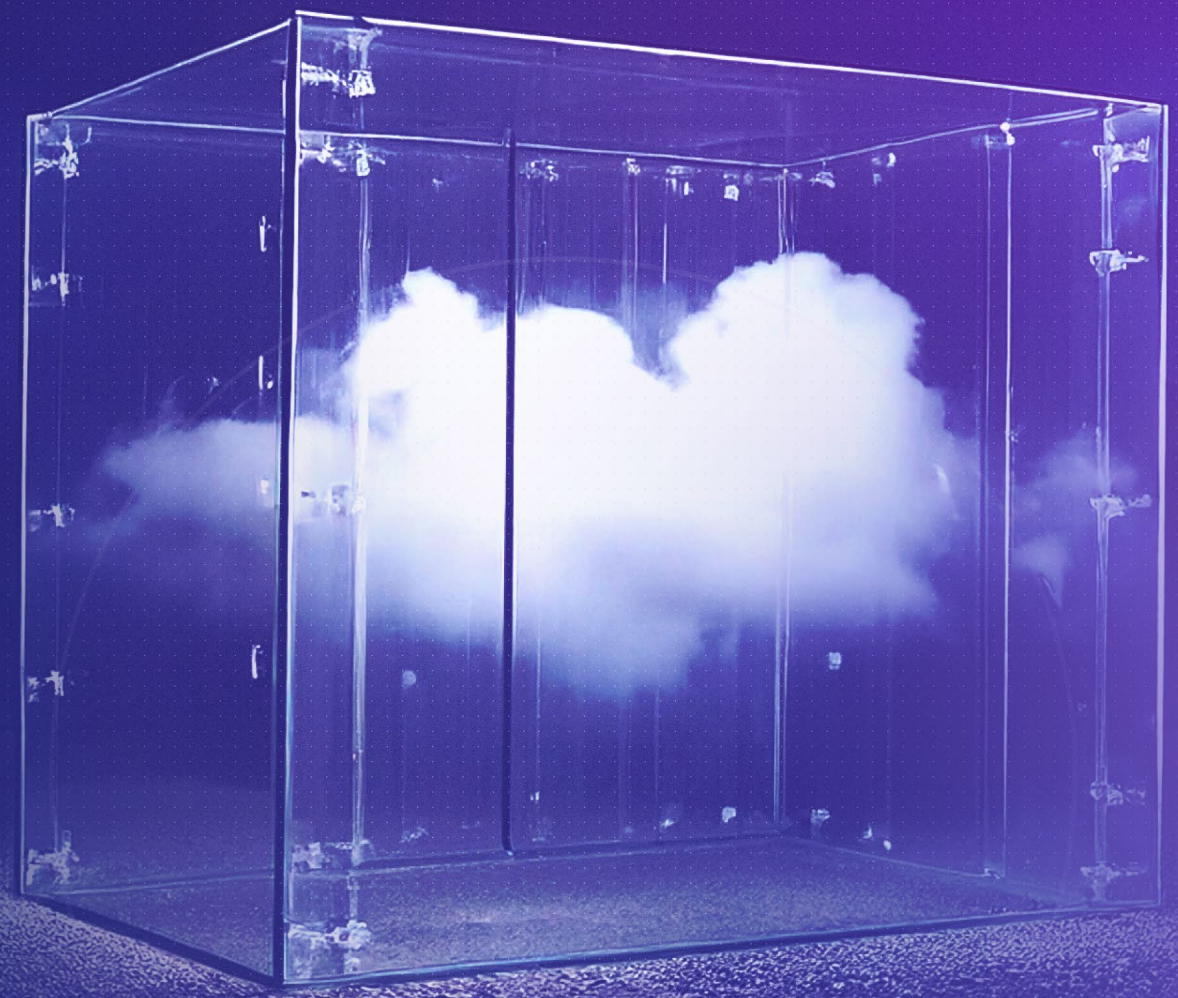
Proactive Hunting

Zero Trust

SentinelOne

RSAC 2025 Conference

Cloud SOC



Federated Data

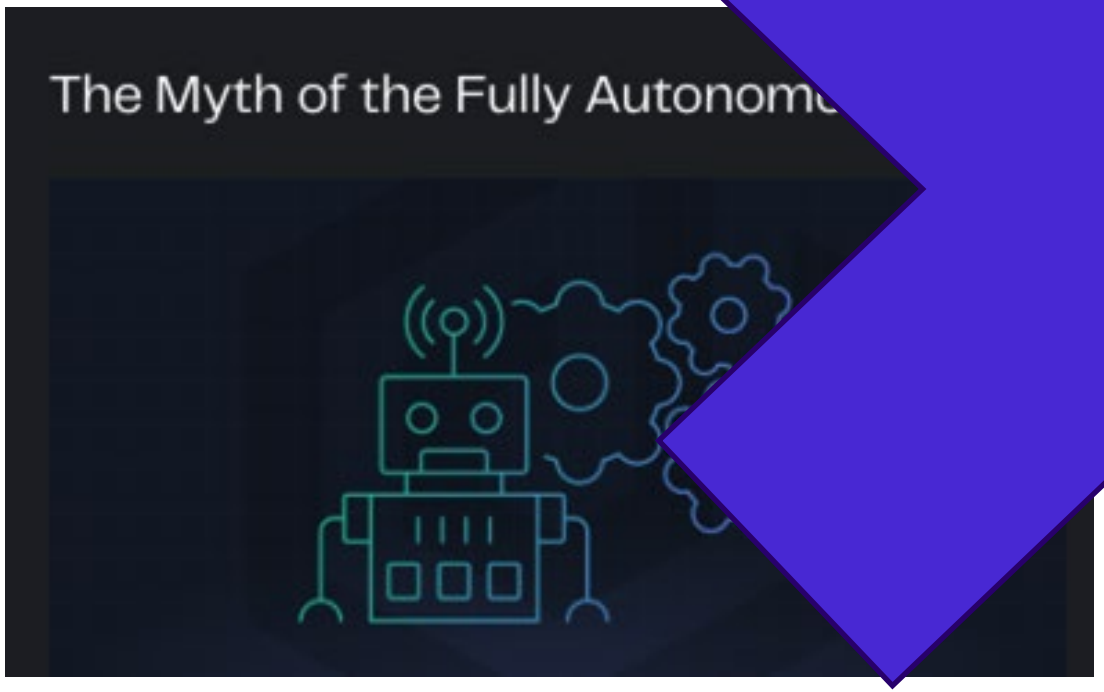
SentinelOne

RSAC 2025 Conference

RSAC 2025 Conference

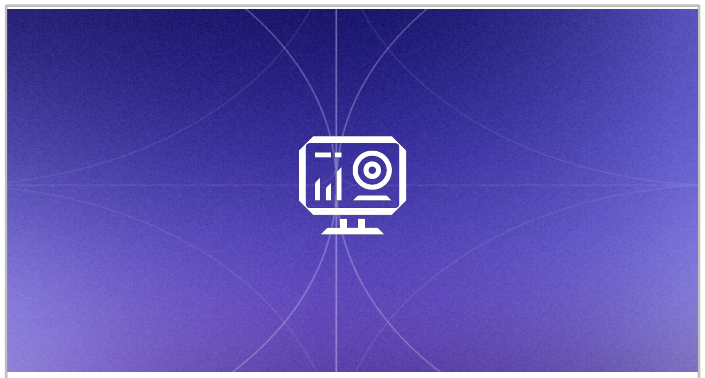
Evolving the SOC

The “Autonomous SOC” Is A Pipe D…

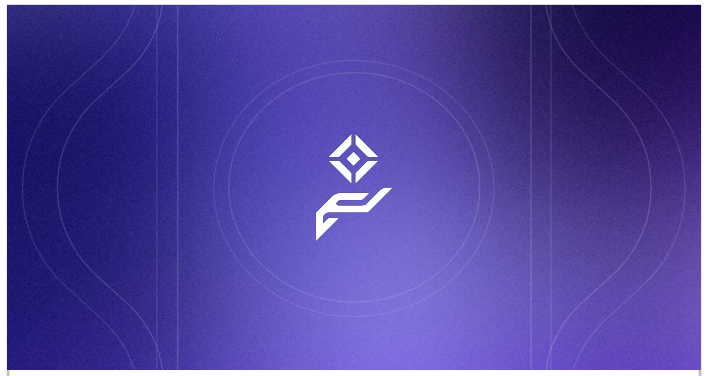


…tomation isn't the right
…olve
We … better detection engineering

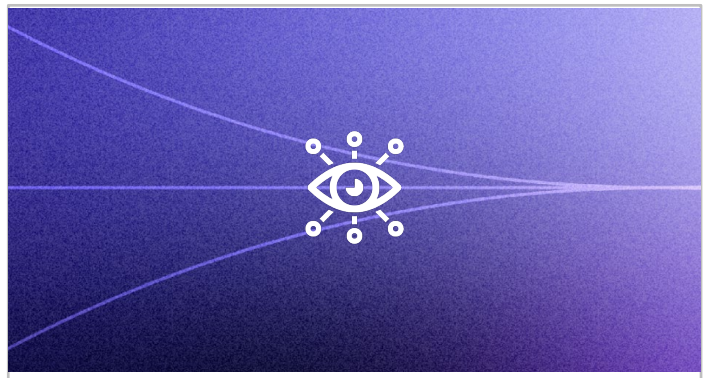
SOC Processes Benefiting from AI



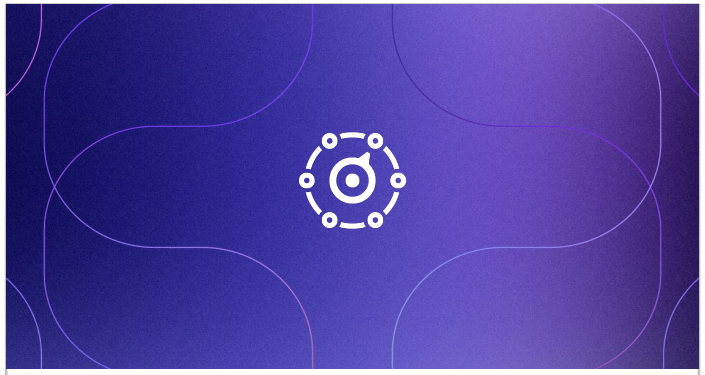
Monitoring



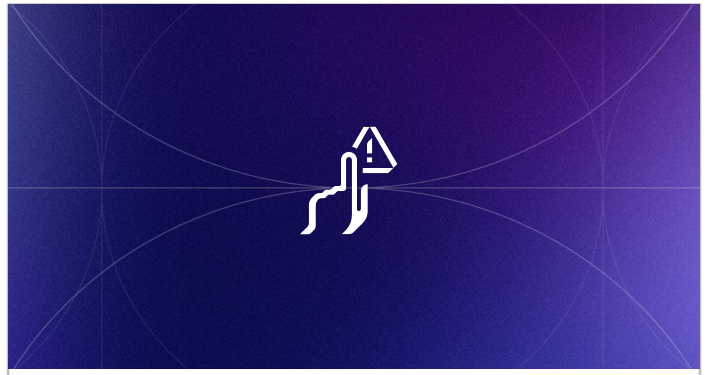
Collecting Evidence



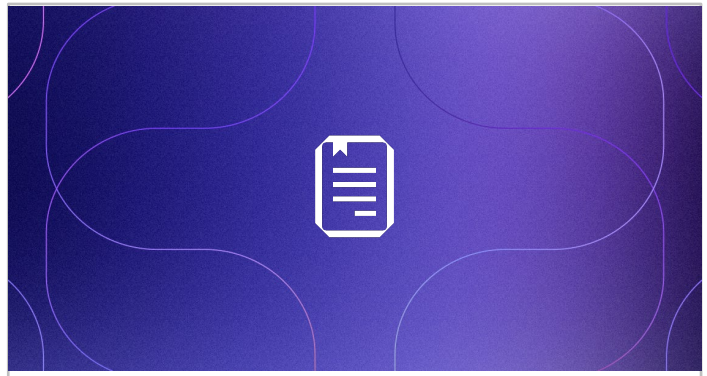
Investigating



Triage



Respond & Remediate



Reporting

The Potential of an Autonomous SOC

Secure Vast and Complex Environments

Attack surfaces are vast, spanning endpoints, networks, and the cloud. AI is required for comprehensive visibility and protection across the entire ecosystem

Accelerate Investigation and Response

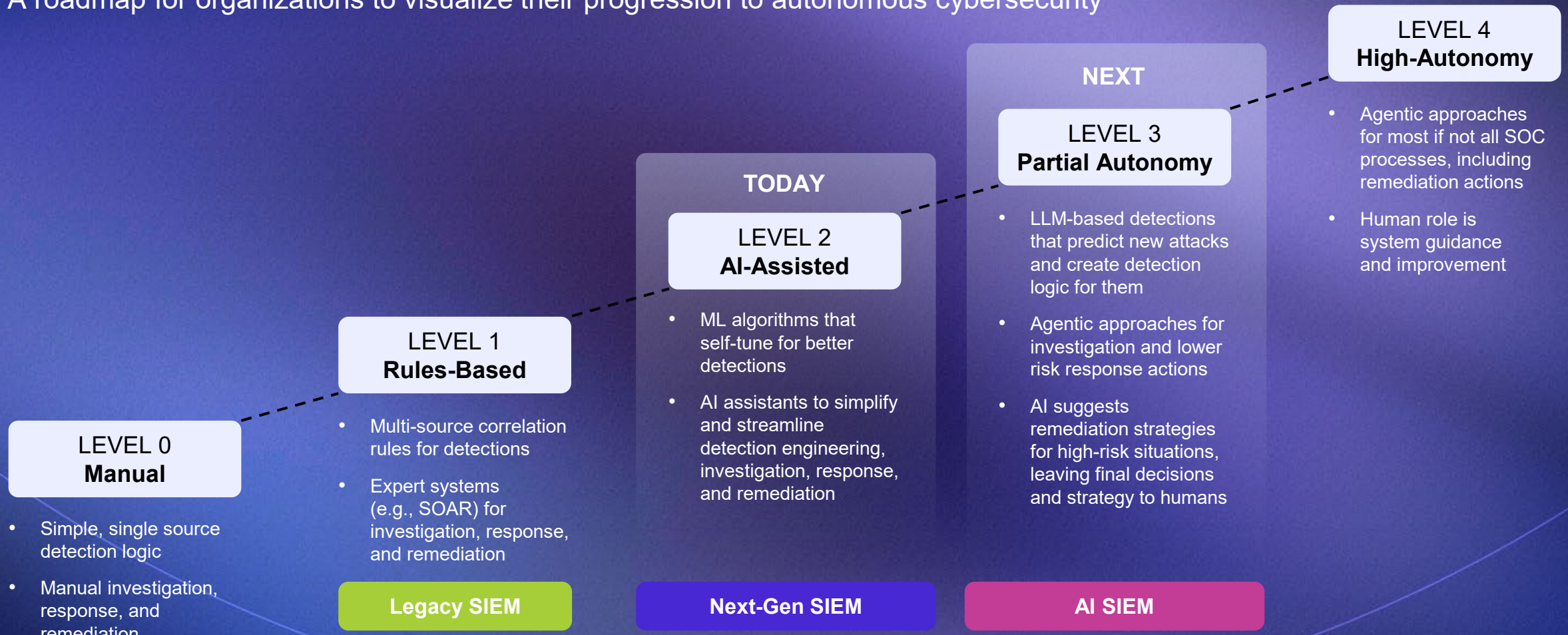
Drastically reduces the time it takes to detect, investigate, and respond to threats. Autonomously correlates events, prioritizes alerts, and provides actionable recommendations.

Real-Time AI-Powered Protection

Protects organizations in real time, identifying and neutralizing threats before they can cause damage.

Future of the SOC: Evolving Toward Autonomous Security

A roadmap for organizations to visualize their progression to autonomous cybersecurity


LEVEL 0
Manual
Simple, single source detection logic
Manual investigation, response, and remediation
LEVEL 1
Rules-Based
Multi-source correlation rules for detections
Expert systems (e.g., SOAR) for investigation, response, and remediation
Legacy SIEM
TODAY
LEVEL 2
AI-Assisted
ML algorithms that self-tune for better detections
AI assistants to simplify and streamline detection engineering, investigation, response, and remediation
Next-Gen SIEM
NEXT
LEVEL 3
Partial Autonomy
LLM-based detections that predict new attacks and create detection logic for them
Agentic approaches for investigation and lower risk response actions
AI suggests remediation strategies for high-risk situations, leaving final decisions and strategy to humans
AI SIEM
LEVEL 4
High-Autonomy
Agentic approaches for most if not all SOC processes, including remediation actions
Human role is system guidance and improvement

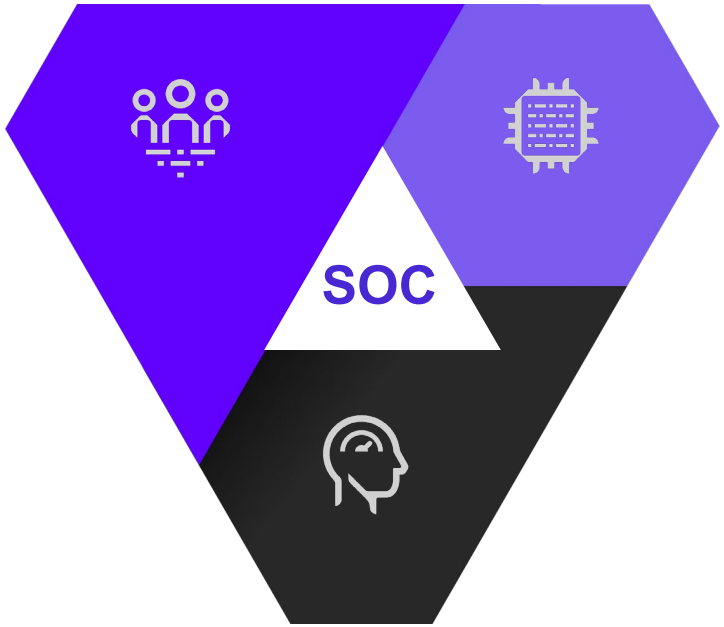
SentinelOne

RSAC 2025 Conference

Key Components of the Autonomous SOC

People

- L3 Security Analysts
- Threat Modeling
- SOC Managers
- AI/ML Experts
- Cloud SOC Analysts



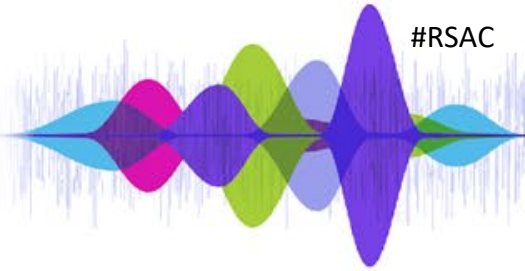
Technology

- AI SIEM
- Hyper Automation
- Agentic AI
- AI Created Threat Intel
- Anomaly and ML Detections

Process

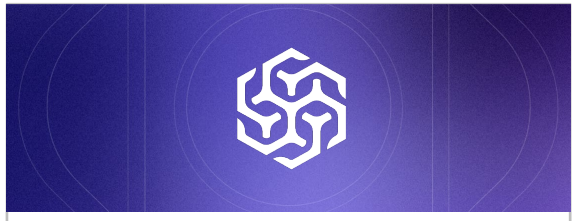
- Automated Playbooks
- Auto Triage & Investigation
- Zero Trust Architecture
- Proactive Threat Hunting

SOC transformation requires the right platform



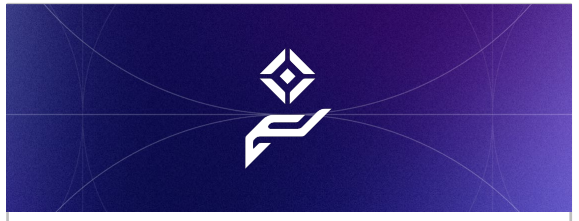
Scalable

Must be architected for petabyte scale. Likely cloud native with auto-scaling capabilities



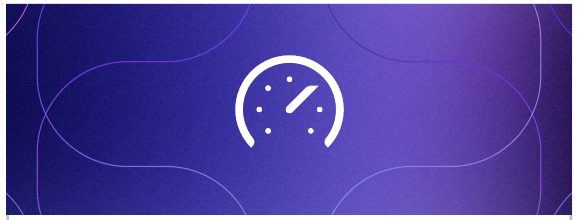
Open & Federated

Platforms must be open and able to ingest data from any tool. API first architectures and pre-built integrations



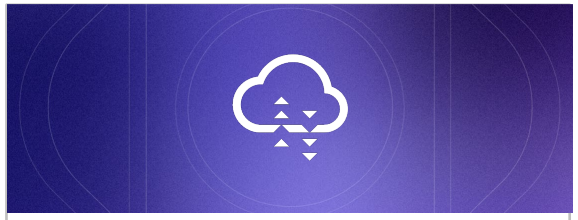
Cost Effective

Data volumes are growing faster than budgets. Need solutions that don't break the bank



Fast

The benefits of AI cannot be realized if it takes took long for it to see and search data



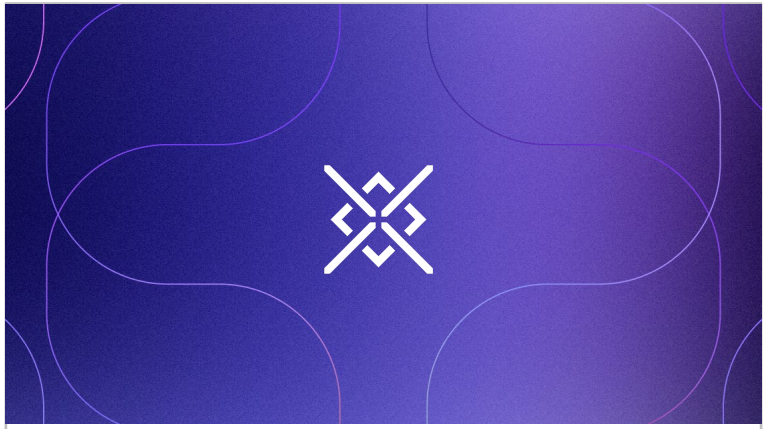
Cloud-Native

Automated, Scalable and built to natively integrate into cloud workflows

Long-Term Retention

Must be able to store data for long periods of time for anomaly and ML detections

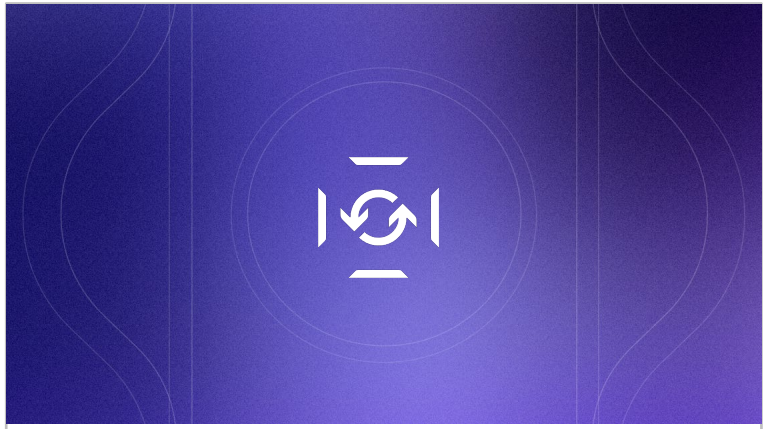
The Need for Speed



Time to Availability

The time takes for an event to be ingested and searchable

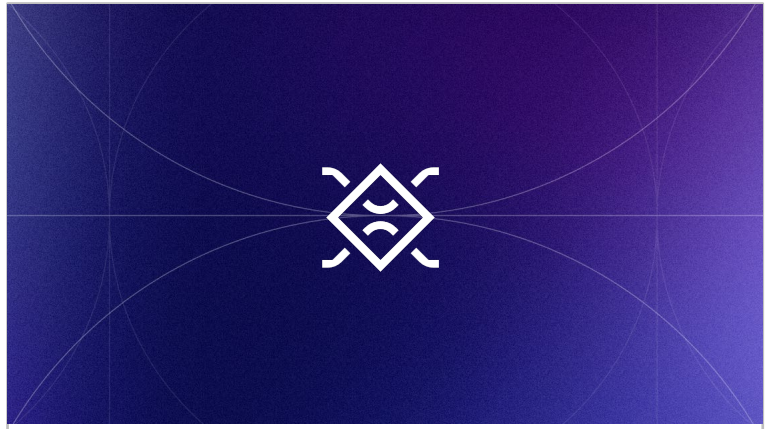
< 10 Seconds



Time to Search

The time it takes to get back results from a query.

< 10 Seconds

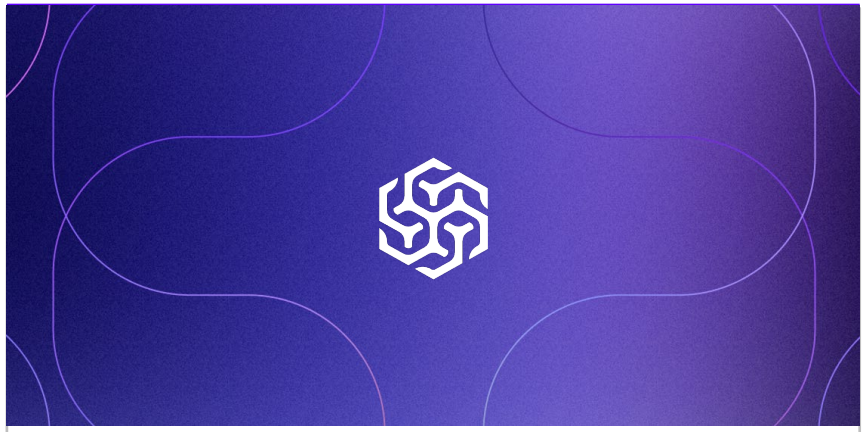


Time to Detect /Respond

The time it takes to fully investigate an incident

<1 Minute

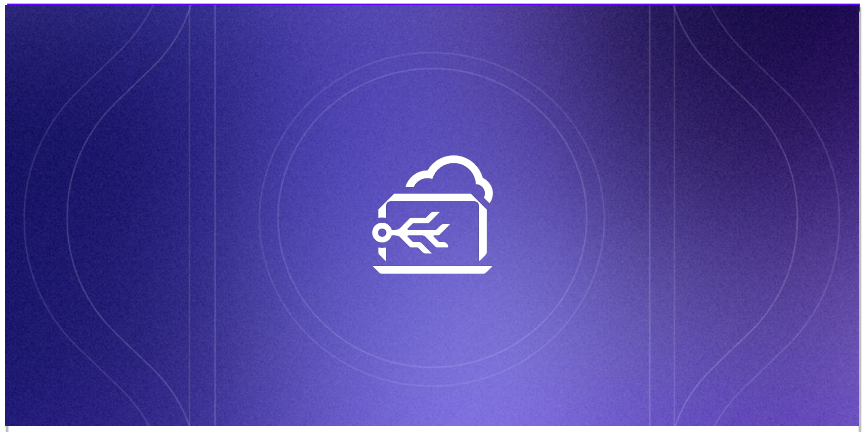
Move from Generative AI to Agentic AI



Generative AI

Generate human-readable content, summaries, and natural-language responses from security data, enabling rapid understanding and analysis

Assist me with my work

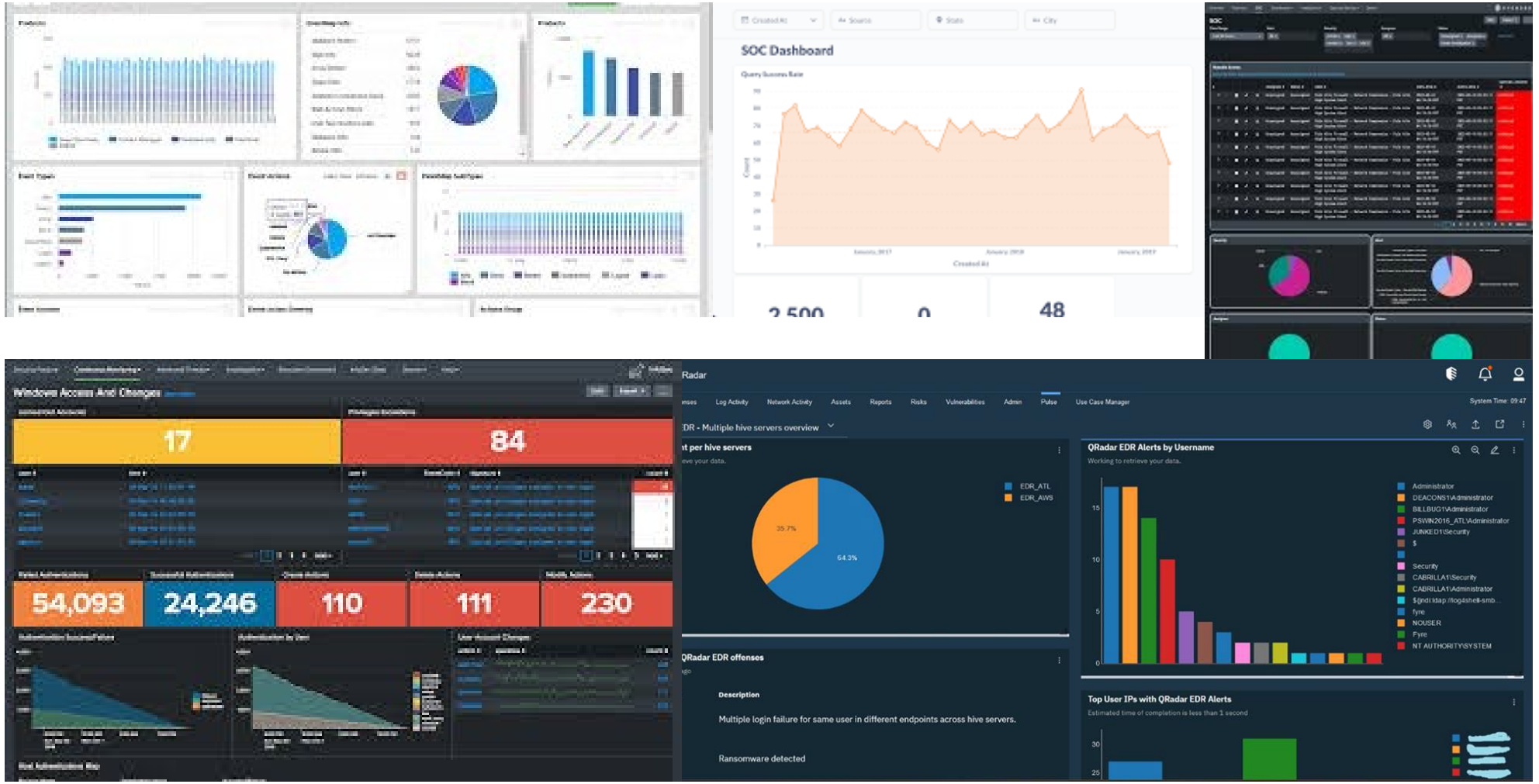


Agentic AI

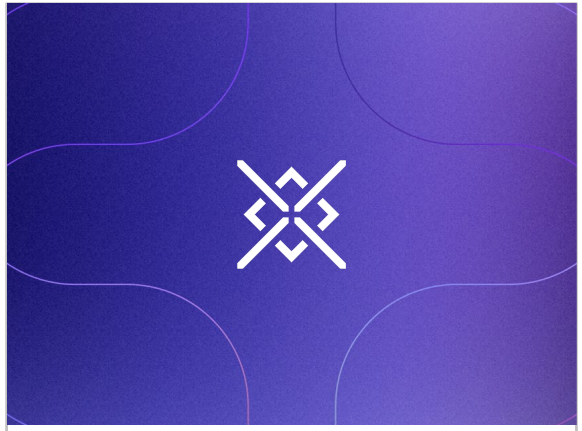
Autonomously performs tasks, proactively identifies next steps, suggests actions, prioritizes activities, and guides decision-making.

Do work for me

Must Evolve SOC Visualizations

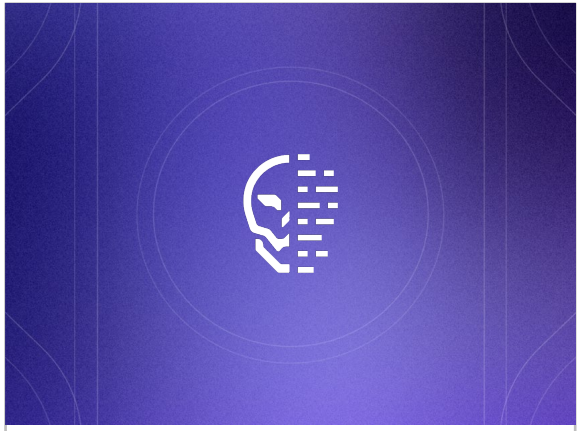


AI Detections



Behavioral

Monitor all activity to detect behaviors that are acting in a malicious or non-standard way

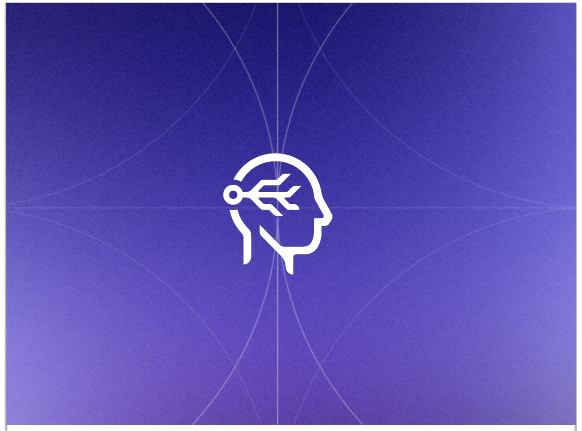


Anomaly

Establish baselines for normal activity and link together with other anomalies to determine a threat

Correlation

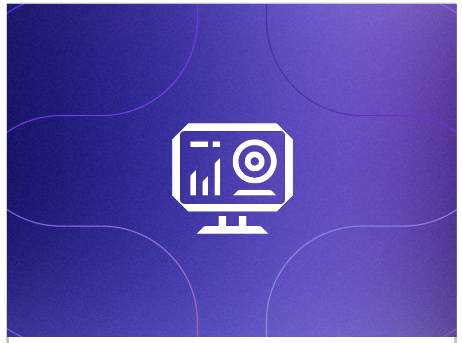
Look at indicators and IOCs across a disparate source of data to find and correlate threats and attacks together



Autonomous AI

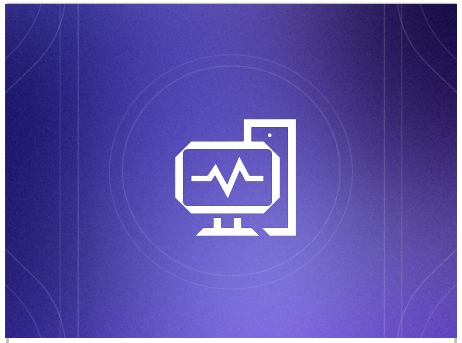
AI innovation drives predictive, real-time defenses that adapt to evolving threats leveraging machine learning, generative AI, and LLMs.

Proactive Security



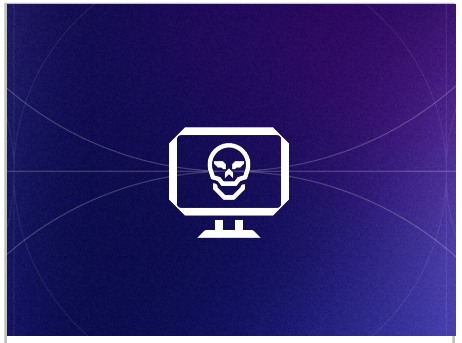
Automated Vulnerability Scanning

Find Vulnerabilities Faster



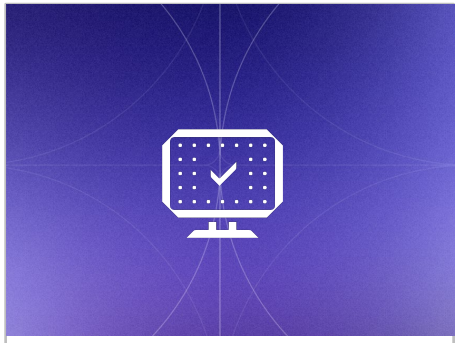
Automated Attack Simulation

Use AI like an Attacker



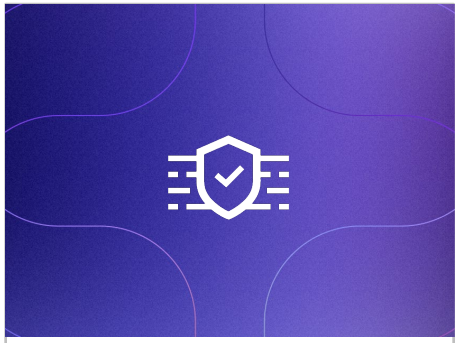
Automated Hunting

Use AI to find Threats Faster



Automated Patching

Reduce Attack Surface



Continuous Posture Management

Identify User Error

Cloud Security Operations Center

Agentless Cloud Security Posture Management	Cloud Infrastructure Entitlement Management	Cloud Data Security
Cloud Native Automation	Cloud Data Lake	Code Scanning & Analysis

Apply: How to start your SOC Evolution

Path 1 (Months, Years)

Transform

- Data Platform
- AI Everywhere
- Automation First
- Threat Hunting
- Detection & Response
- Cloud SOC

- Time-Consuming & Costly
- Better prepared for future threats & Large Efficiency gains

Path 2 (Days, Weeks)

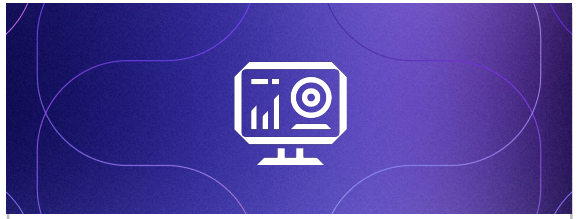
Optimize

- Augment with a Data Lake
- Build Detection Content
- XDR for Automation
- Start a Hunting Program
- Move to platforms
- Get Cloud Visibility

- Less Costly & Easier to implement
- Small Detection and process Improvements

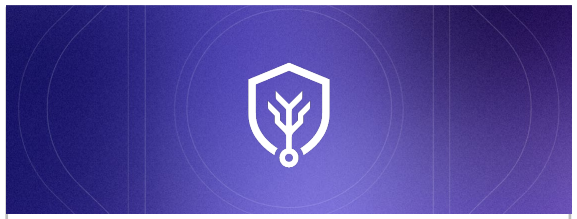
Focus on Fixing What's Broken

Final Takeaways



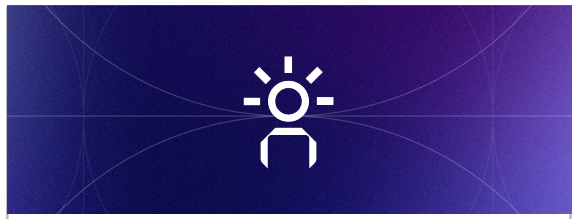
AI Evolution is Now

Increasingly sophisticated and capable of handling the entire cybersecurity operation.



Levels of Autonomy

The appropriate level of autonomy will vary based on organizational needs and business objectives.

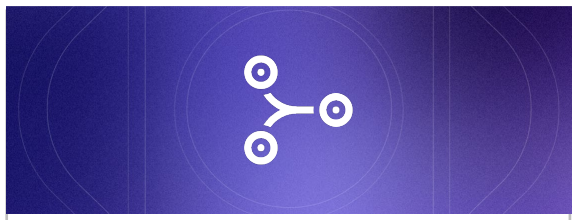


The Human Shift

Humans should continue to learn how to perform dynamic security tasks themselves. Shift from Triage to tactical strategy

Set New Benchmarks

AI will set new benchmarks in three key areas: Speed, Expertise, and Volume.



Deprecated SOC Tiers

The typical tiered SOC structure is changing and will soon become obsolete.

Strategic Focus

Create a vision for where you want your SOC to be and build a path to get there based on your organization

RSAC™ 2025 Conference

Many Voices.
One Community.

Questions?